AFOSR 820

IMM-NYU 282
JUNE 1961

NEW YORK UNIVERSITY
INSTITUTE OF
MATHEMATICAL SCIENCES

Extensions and Corollaries of Recent Work on Hilbert's Tenth Problem

MARTIN DAVIS

PREPARED UNDER
CONTRACT NO. AF49(638)-777
MATHEMATICAL SCIENCES DIRECTORATE
AIR FORCE OFFICE OF SCIENTIFIC RESEARCH

AFOSR 820

IMM-NYU 282
June 1961

New York University
Institute of Mathematical Sciences

EXTENSIONS AND COROLLARIES OF RECENT WORK ON HILBERT'S TENTH PROBLEM

Martin Davis

ABSTRACT: The theorem that every recursively enumerable set is exponential Diophantine is improved; a sharp form is given of Kleene's normal form theorem, a problem of Quine is proved recursively unsolvable.

The research reported in this document has been sponsored by the Mathematical Sciences Directorate, Air Force Office of Scientific Research, Washington 25, D, C., under Contract No. AF 49(638)-777.

This paper consists of three separate notes related only in that each of the three either extends or employs the results of [2], with which acquaintance is assumed,

1. A sharpening of Kleene's normal form theorem.

By a form of Kleene's normal form theorem[1] we may understand an assertion stating:

Theorem. There is a function $U(y)$ *and a predicate* $T(z,x,y)$ *both belonging to the class* Q *such that a function* $f(x)$ *is partially computable if and only if for some number* e:

$$f(x) = U\big(\min_y T(e,x,y)\big) \quad .$$

In its original form, this result was stated with Q the class of primitive recursive functions and predicates. It is well-known[2] that smaller classes Q suffice. We wish to point out here that (assuming variables to range over the positive integers) we may take for Q the following extremely modest class:

(1) A function f belongs to Q if and only if f can be obtained by repeated application of the operation of composition to the functions: 2^x, $x \cdot y$, $N(x) = 0$, $U_i^n(x_1,\ldots,x_n) = x_i$, $K(x)$, $L(x)$, where $K(x)$, $L(x)$ are recursive pairing functions.

(2) A predicate $R(x_1,\ldots,x_n)$ belongs to Q if:

$$R(x_1,\ldots,x_n) \longleftrightarrow f(x_1,\ldots,x_n) = g(x_1,\ldots,x_n)$$

where $f,g \in Q$.

In fact, we may even take $U(y) = K(y)$

To see this we begin by noting thay by Corollary 5 of [2], (or rather the immediate extension thereof to predicates), we

have:

$$\bigvee_y T_2(z,x,u,y) \longleftrightarrow \bigvee_{x_1,\ldots,x_n} P(z,x,u,x_1,\ldots,x_n,2^{x_1},\ldots,2^{x_n}) = 0 \quad .$$

$$\longleftrightarrow \bigvee_{x_1,\ldots,x_n} \left\{ \sum_{j=1}^{m} f_j(z,x,u,x_1,\ldots,x_n,2^{x_1},\ldots 2^{x_n}) \right.$$

$$= \sum_{j=1}^{m} g_j(z,x,u,x_1,\ldots,x_n,2^{x_1},\ldots,2^{x_n})$$

where $f_j, g_j \in Q$, $j = 1,2,\ldots,m$.

Now, using the fact

$$\sum A_j = \sum B_j \longleftrightarrow 2^{\sum A_j} = 2^{\sum B_j} \quad ,$$

$$\longleftrightarrow \prod 2^{A_j} = \prod 2^{B_j} \quad ,$$

we see that

$$\bigvee_y T_2(z,x,u,y) \longleftrightarrow \bigvee_{x_1,\ldots,x_n} R(z,x,u,y,x_1,\ldots,x_n)$$

where $R \in Q$.

Now, let $q_1(t) = K^{n-1}(t)$,

$$q_j(t) = L\big(K^{n-j}(t)\big) \, , \quad j = 2,3,\ldots,n \quad ,$$

where the exponent on K indicates iterated application, so that $q_j(t) \in Q$, $j = 1,2,\ldots,n$. Thus

$$\bigvee_y T_2(z,x,u,y) \longleftrightarrow \bigvee_t R\big(z,x,u,y,q_1(t),\ldots,q_n(t)\big)$$

$$\longleftrightarrow \bigvee_t S(z,x,u,y,t)$$

where $S \in Q$.

Let $f(x)$ be any partially computable function. Then the predicate $u = f(x)$ is semicomputable (recursively enumerable). Hence, for some e, $u = f(x) \iff \bigvee_{y} T_2(e,x,u,y)$

$$\iff \bigvee_{t} S(e,x,u,t) \quad .$$

Finally,

$$f(x) = K\left(\min_{y} S\left(e,x,K(y),L(y)\right)\right) \quad .$$

So, we have derived Kleene's normal form theorem with

$$T(z,x,y) \iff S\left(z,x,K(y),L(y)\right)$$

and

$$u(y) = K(y) \quad .$$

2. <u>Negative solution to a problem of Quine</u>. In [4], Quine proposed the following problem:

Let us consider schemata constructed from the following ingredients:

Numerals, variables ranging over the non-negative integers, the symbols of sum, product and power, = , and the truth-function signs.

Such a schema is called <u>valid</u> if it becomes a true sentence whenever all of the variables occurring in it are replaced by numerals. The proposed problem is to give an algorithm for determining whether or not a given schema of this kind is valid.

We note here that the <u>recursive unsolvability of this problem</u>

follows directly from the results of [2]. For, to each exponential Diophantine equation, E = F, there corresponds, mechanically, a "translation": $\Gamma = \Delta$ which is a schema of the kind being considered. Moreover, E = F has a solution if and only if the schema $\sim(\Gamma = \Delta)$ is not valid. Hence, an algorithm for solving Quine's problem could be used to solve the decision problem for exponential Diophantine equations. But, by [2], there is no algorithm for solving this latter problem. Hence, Quine's problem is likewise unsolvable.

<u>3. Diophantine representation of recursively enumerable sets in terms of a single predicate of exponential growth</u>. A predicate $\rho(u,v)$ will be called a <u>Julia Robinson predicate</u> if:

(1) $\rho(u,v) \rightarrow v \leqq u^u$

(2) For each $k > 0$, there are u,v such that:

$$\rho(u,v) \wedge v > u^k \quad .$$

We shall prove the:

<u>Theorem</u>. <u>Let</u> S <u>be a recursively enumerable set. Then, there is a polynomial</u> P <u>such that</u>:

$$S = \left\{ x \,\middle|\, \bigvee_{x_1,\ldots,x_n,u,v} [P(x,x_1,\ldots,x_n,u,v) = 0 \wedge \rho(u,v)] \right\}$$

<u>for every Julia Robinson predicate</u> $\rho(u,v)$.

Since, e.g. the predicate $v = 2^u \wedge u > 1$ is a Julia Robinson predicate, we have the

<u>Corollary 1</u>. Let S be a recursively enumerable set. Then, for some polynomial P,

$$S = \left\{ x \,\middle|\, \bigvee_{x_1,\ldots,x_n,u} P(x,x_1,\ldots,x_n,u,2^u) = 0 \right\} .$$

This generalizes Corollary 5 of [2]. Moreover, the proof of Corollary 6 of [2], if applied to the present Corollary 1 instead of to Corollary 5 of [2], yields:

Corollary 2. *For every recursively enumerable set* S *there is a function* $P(x_1,\ldots,x_n,u,2^u)$, *where* P *is a polynomial, whose range (for positive integer value of the variables) consists of the members of* S *together with the non-positive integers.*

If in particular we choose for S, the set of positive primes, we obtain a curious "prime-representing" function.

It remains to prove the theorem stated above. In doing so we generalize the methods, relating to Pell's equation, of [5].[3] We recall the notation $x = a_n$, $y = a'_n$ for the successive solutions of the Pell equation $x^2 - (a^2 - 1)y^2 = 1$.

Lemma 1. There is a Diophantine predicate $\psi(a,u)$ such that:

(1) $\psi(a,u) \longrightarrow u \geqq a^a$

(2) $a > 1 \longrightarrow \bigvee_u \psi(a,u)$.

Proof. This is a weakening of Lemma 8 of [5].

Lemma 2. There is a Diophantine predicate $D(c,y,z)$ such that

(1) $a > c \wedge D(c,y,z) \longrightarrow a > y^z$

(2) $\bigwedge_{y,z} \bigvee_c D(c,y,z)$

Proof. Let

$$D(c,y,z) \longleftrightarrow \bigvee_b [b > y \wedge b > z \wedge \psi(b,c)] .$$

Then,

$$a > c \wedge D(c,y,z) \longrightarrow \bigvee_b [a > c \geqq b^b > y^z] .$$

Lemma 3. If $y > 1$ and $a > y^z$ then $y^z = [u/a_z]$ where[4] u is chosen as a solution of

$$u^2 - (a^2y^2 - 1)v^2 = 1 \quad \text{for which} \quad a_z \leqq u \leqq a \cdot a_z .$$

Proof. By Lemma 9 of [5], $y^z = [(ay)_z/a_z]$, and by Lemma 10, the number u is precisely $(ay)_z$.

Lemma 4.

$$\bigwedge_{i \leqq m} (x_i = y_i^{z_i}) \longleftrightarrow \bigvee_{r_1,\ldots,r_m} \bigwedge_{i \leqq m} E(r_i,x_i,y_i,z_i,a) \wedge \bigwedge_{i \leqq m} (r_i = a_{z_i})]$$

where E is a Diophantine predicate and where $a > c_1, c_2, \ldots, c_m, z_1, \ldots, z_m$ with the $c_1, \ldots, c_m$ satisfying $D(c_i, y_i, z_i)$.

Proof. We need only take

$$E(r_i,x_i,y_i,z_i,a) \longleftrightarrow \bigvee_{u,v} [(u^2 - (a^2y_i^2 - 1)v^2 = 1)$$

$$\wedge\ r_i \leqq u \leqq a \cdot r_i \wedge r_i x_i \leqq u < r_i(x_i + 1)] \vee [x_i = y_i = 1] .$$

Lemma 5. If $1 < r < a_a$ and $a > z$, then

$$r = a_z \longleftrightarrow \bigvee_s [r^2 - (a^2 - 1)\big(z + s(a - 1)\big)^2 = 1] .$$

Proof. This follows from Lemma 7 of [5].

Lemma 6.

$$\bigwedge_{i \leq m} (x_i = y_i^{z_i}) \Longleftrightarrow \bigvee_{a,d} [F(x_1,\ldots,x_m,y_1,\ldots,y_m,z_1,\ldots,z_m,a,d) \wedge \rho(a,d)]$$

where F is a Diophantine predicate and ρ may be any Julia Robinson predicate.

Proof. We claim that, using the notation of Lemma 4:

$$\bigwedge_{i \leq m} (x_i = y_i^{z_i}) \Longleftrightarrow \bigvee_{r_1,\ldots,r_m} \bigvee_{a} \Big\{ \bigwedge_{i \leq m} \Big[E(r_i,x_i,y_i,z_i,a)$$

$$\wedge (a > z_i) \wedge \bigvee_{s_i} [r_i^2 - (a^2 - 1)(z_i + s_i(a - 1))^2 = 1]\Big]$$

$$\wedge \bigvee_{c_1,\ldots,c_m} [\bigwedge_{i \leq m} (D(c_i,y_i,z_i) \wedge a > c_i)]$$

$$\wedge \bigvee_{d} [r_1,\ldots,r_m \leq d \wedge \rho(a,d)] \quad .$$

For, if the right-hand side holds, then $r_1,\ldots,r_m \leq d \leq a^a < a_a$ so that by Lemma 5, $r_i = a_{z_i}$, and finally, by Lemma 6, $x_i = y_i^{z_i}$. Conversely, if the left-hand side holds choose c_i so that $D(c_i,y_i,z_i)$ is satisfied, then let $z = \max_{i \leq m} z_i$, and choose a,d so that $a > c_i$, $a > z$, $\rho(a,d)$, and $d > a_z$. Then,

$$r_i = a_{z_i} \leq a_z < d \quad ,$$

and the result follows by Lemma 4 and 5.

Lemma 7. Let S be a recursively enumerable set. Then, there is a polynomial P such that:

$$S = \left\{ x \,\middle|\, \bigvee_{x_1,\ldots,x_m} \bigvee_{y_1,\ldots,y_m} \bigvee_{z_1,\ldots,z_m} [P(x,x_1,\ldots,x_n,y_1,\ldots,y_m,z_1,\ldots,z_m) = 0] \wedge \bigwedge_{i \leq m} (x_i = y_i^{z_i}) \right\} .$$

Proof. This lemma is essentially a restatement of the main result of [2], namely that every recursively enumerable set is exponential Diophantine.

The theorem now follows at once from Lemmas 6 and 7.

Footnotes

1. Cf. [1] or [3].
2. Cf. [3] and [6].
3. However, we are following [2] rather than [5] in taking variables to have the positive integers (rather than the non-negative integers) as their range.
4. [...] here means, as usual, "the greatest integer $\leqq$ ... ."

References

[1] Martin Davis, Computability and unsolvability, McGraw-Hill, 1958.

[2] Martin Davis, Hilary Putnam, and Julia Robinson, The decision problem for exponential Diophantine equations. Annals of Mathematics, forthcoming.

[3] S. C. Kleene, Introduction to metamathematics, D. Van Nostrand Company, Inc., 1952.

[4] W. V Quine, On decidability and completeness, Synthese, vol. VII (1948-9), pp. 441-46.

[5] Julia Robinson, Existential definability in arithmetic, Transactions of the American Mathematical Society, vol. 72 (1952), pp. 437-449.

[6] Raymond Smullyan, Theory of formal systems, Annals of Mathematics Studies, 1961.

DISTRIBUTION LIST AIR FORCE OFFICE OF SCIENTIFIC RESEARCH
MATHEMATICAL SCIENCES DIRECTORATE
(ONE COPY UNLESS OTHERWISE NOTED)

ALABAMA

Commander
Army Rocket & Guided Missile Agency
ATTN: ORDXR-OTL
Redstone Arsenal, Alabama

BELGIUM

Commander (3)
European Office, ARDC
47 Rue Cantersteen
Brussels, Belgium

CALIFORNIA

Applied Mathematics & Statistics Laboratory
Stanford University
Stanford, California

Department of Mathematics
University of California
Berkeley, California

Commander
Air Force Flight Test Center
Attn: Technical Library
Edwards Air Force Base, California

The Rand Corporation (2)
Technical Library
1700 Main Street
Santa Monica, California

Commander
1st Missile Division
ATTN: Operations Analysis Office
Vandenburg Air Force Base, California

CONNECTICUT

Department of Mathematics
Yale University
New Haven, Connecticut

DISTRICT OF COLUMBIA

Office of Naval Research (2)
Department of the Navy
ATTN: Code 432
Washington 25, D. C.

Director
Department of Commerce
Office of Technical Services
Washington 25, D. C.

Administrator (6)
National Aeronautics & Space Administration
ATTN: Documents Library
1520 H Street, N. W.
Washington 25, D. C.

Library
National Bureau of Standards
Washington 25, D. C.

Data Processing Systems Division
National Bureau of Standards
ATTN: Mr. Russell A. Kirsch
Washington 25, D. C.

Applied Mathematics Division
National Bureau of Standards
Washington 25, D. C.

Headquarters, USAF
Assistant for Operations Analysis
Deputy Chief of Staff, Operations, AFOOA
Washington 25, D. C.

Commander (2)
Air Force Office of Scientific Research
ATTN: SRM
Washington 25, D. C.

Director
U. S. Naval Research Laboratory
Attn: Library
Washington 25, D. C.

(2) [illegible]
Attn: [illegible] Library
Washington 25, D. C.

National Bureau of Standards
[illegible]
Washington 25, D. C.

[illegible]
Washington 25, D. C.

ILLINOIS

[illegible]

INDIANA

Department of Mathematics
Purdue University
Lafayette, Indiana

MARYLAND

Institute for Fluid Dynamics and Applied Mathematics
University of Maryland
College Park, Maryland

[illegible]
Baltimore, Maryland

[illegible]

MASSACHUSETTS

[illegible]
Cambridge, Massachusetts

[illegible]

NEBRASKA

Commander
Strategic Air Command
ATTN: Operations Analysis
Offutt Air Force Base
Omaha, Nebraska

NEW JERSEY

The James Forrestal Research
Center Library
Princeton University
Princeton, New Jersey

Library
Institute for Advanced Study
Princeton, New Jersey

Department of Mathematics
Fine Hall
Princeton University
Princeton, New Jersey

Commanding General
Signal Corps Engineering Laboratory
ATTN: SIGFM/EL-RPO
Ft. Monmouth, New Jersey

NEW MEXICO

Commander
Air Force Missile Development
Center
ATTN: Technical Library, HDOI
Holloman Air Force Base, New Mexico

Commander
Air Force Special Weapons Center
ATTN: Technical Library, SWOI
Kirtland Air Force Base
Albuquerque, New Mexico

NEW YORK

Professor J. Wolfowitz
Mathematics Department
White Hall
Cornell University
Ithaca, New York

Department of Mathematics
Syracuse University
Syracuse, New York

Institute for Mathematical
Sciences
New York University
ATTN: Professor M. Kline
25 Waverly Place
New York 3, New York

Institute for Aeronautical
Sciences
ATTN: Librarian
2 East 64th Street
New York 16, New York

NORTH CAROLINA

Department of Mathematics
University of North Carolina
Chapel Hill, North Carolina

Department of Statistics
University of North Carolina
Chapel Hill, North Carolina

Office of Ordnance Research (2)
Box CM
Duke Station
Durham, North Carolina

Department of Mathematics
Duke University
Duke Station
Durham, North Carolina

OHIO

P. O. Box AA
Wright-Patterson Air Force Base
Ohio

Commander
Wright Air Development Division
ATTN: WCOSI
Wright-Patterson Air Force Base
Ohio

Commander
Aeronautical Research
Laboratories
ATTN: Technical Library
Wright-Patterson Air Force Base
Ohio

USAF Institute of Technology (2)
Library
ATTN: MCLI-ITLIB
Building 125, Area B
Wright-Patterson Air Force Base
Ohio

PENNSYLVANIA

Department of Mathematics
Carnegie Institute of Technology
Pittsburgh, Pennsylvania

Department of Mathematics
University of Pennsylvania
Philadelphia, Pennsylvania

TENNESSEE

AEDC Library
ARO, Inc.
Arnold AF Station, Tennessee

U. S. Atomic Energy Commission
Technical Information Service
Extension
P. O. Box 62
Oak Ridge, Tennessee

TEXAS

Applied Mechanics Reviews (2)
Southwest Research Institute
8500 Culebra Road
San Antonio 6, Texas

Department of Mathematics
Rice Institute
Houston, Texas

VIRGINIA

Armed Services Technical (2)
Information Agency
ATTN: TIPDR
Arlington Hall Station
Arlington 12, Virginia

WISCONSIN

Department of Mathematics
University of Wisconsin
Madison, Wisconsin

Mathematics Research Center,
U. S. Army
ATTN: R. E. Langer
University of Wisconsin
Madison, Wisconsin